IPASJ International Journal of Computer Science (IIJCS)
Web Site: http://www.ipasj.org/IIJCS/IIJCS.htm
A Publisher for Research Motivation ....
Email: editoriijcs@ipasj.org
Volume 4, Issue 6, June 2016
ISSN 2321-5992

Security Breaches in MANET: A State-of-Art

Prachi Sharma[1], Prof.Kalpana Rai,[2]Prof.Deepak Jain[3] and Prof. B. L. Rai[4]

[1]Student,Dept. of Computer Science & Engineering, JNCT, Bhopal,INDIA

[2](Guide)Dept. of Computer Science & Engineering, JNCT, Bhopal, INDIA

[3](HOD)Dept. of Computer Science & Engineering, JNCT, Bhopal, INDIA

[4](Dean)Dept. of Computer Science &Engineering,JNCT,Bhopal, INDIA

ABSTRACT

Mobile Adhoc Networks have become a part and parcel of technology advancements due to its working as autonomous system. MANET networks are very susceptible to several kinds of attacks and risk because of its identical features such as the Shared physical medium, dynamic topology, distributed operations and many more. There are several attacks that influence the working of the MANETS' like the denial of service which is very usually used to affect the network is one of the various types of attacks in the MANETS. Jellyfish attack has achieved its name currently in attack schemes in the MANET. JellyFish Attack achieves the end to end congestion control mechanism of Transmission Control Protocol (TCP). It then refers the potential solution to prevent the mechanism of security that consists of integrity, availability, authentication and non refusal. These issues related to securities are well referred if one may give methods which are relevant for the key distribution, authentication, and intrusion detection in MANETS. Also various attacks in MANET will get discussed in this paper.

Keywords: Jellyfish attack ,blackhole attack. Dos attack, MANET

1. INTRODUCTION

The upcoming generation of the wireless communication systems, there will always be a requirement for the fast deployment of the autonomous users of mobile. Important examples consist ofbuilding survivable, dynamic, efficient communication for the rescue/emergency operations, military networks andefforts for disaster relief. These scenarios of network neverdepend on the centralized and arranged connectivity, and may be assumed as the applications of the **MobileAd Hoc Networks.** Mobile ad-hoc networks or called as "short live" networks work in the area where fixedinfrastructure is absent. They providefast and efficient deployment of network in the situations in which it is otherwise not possible. In MANET, Ad-hoc is a Latin word, that means "for this or for this only."

MANET is aself-determining system of theportableterminalslinked by wireless connections; everyterminalwork as an end system and also a router for the allother terminals in network.In the MANET all terminals are free to leave andjoin the network, also known as open network boundary.All theintermediaryterminals in between the source and the destination participate in routing, and also known as hop-by-hop communications. As the communication medium is wireless andeveryterminal will receive the packets in itswireless range, then either it has been destination of the packets or not. Because of these features, every terminalmay easily received access to the other terminals packets or entersin the network the fault packets.

Therefore, securing the MANET against malignant behaviors and terminals became one of the mostimportant issues in MANET [1].The link between the terminals whenever gets break, the affected terminals request for new routes and hence the new links are generated. MANETS have property in which terminals move freely and can randomly organize themselves that makes this network expandable in the nature. The properties of MANETS have brought tremendous applications in existence.

Applications such as automated battlefields,emergency services and various relief activities, search and recovery operations and recoveries from disaster, commercial and civilian services,Context aware services. MANETS operates on the TCP/IP frameworkto have the connectivity in between theterminals. The traditional TCP/IPmodel is modified orredefined to remunerate the MANETS mobility to have the better functionality. Eachterminalneeds to be assured that theconveyed credentials and identity to the recipient terminals are not adjusted. Hence it is necessary to give the security architecture to protect the ad hoc networking.They detect that several existingattacks have few featurescommon and have been classified into thevarious attacks depended on their insignificant differences.

MANETS work on TCP/IP structure in order to haveconnectivity between terminals. The traditional TCP/IP model isredefined or modified in order to compensate the MANETSmobility in order to have better functionality. RoutingProtocols such as Dynamic source Routing (DSR),Destination Sequenced Distance Vector Protocol (DSDV), Adhoc on Demand Distance Vector (ADOV) are used forforwarding the packets from one terminal to another and toestablish the network connectivity. [2]

2. BACKGROUND

2.1MANET

A fundamental wireless network has a framework with the constant base stationsfor the mobile network hosts systems and/or portable networks. As thecalculating devices are becoming smaller and joined into several systems, like vehicles,phones,homes,sensors, health care systems, and military equipment etc. the pattern is forwarding towards anuniversalwithout infrastructure and self-organizing wireless networks, like*mobilead hoc networks* (MANETs). In MANET,eachhost of network is also a type of base station for the otherhosts of network and hence the network interaction can be created on the demand of without any need for constantequipment in network. Whereas MANETs allowsseveralinterestingcharacteristics for the further interaction in the network they also discoverseveralissuesrelated to [10]:

-speed
- unicast routing
- dynamic network topology
- multicast routing
- scalability
- frequency of updates or network overhead
- energy efficient/power aware routing
- mobile agent based routing
- Quality of Service (QoS)
- secure routing

MANETs needs central control and earlierarrangement,so that the issues related to security are dissimilar and hence requires different security mechanisms than in conventional networks.Wireless links in MANETs make them more susceptible to the attacks. For the hackers it is easier to attack these networks easilyand thus gain access to confidential information. They alsocan attackdirectly to the network to delete the messages, add malignant messages, or masquerade as a terminal. This violates the network goals of availability, integrity,confidentiality, authenticity and authorization[15].

Wireless network of MANET is taken as more susceptible to the attacks as compareto the wired networks due to there are variousissueswhich will be analyzed in this paper. In MANET the security isa vital issue, as in MANET the communication is done in groups.Also the senders and the receiversare many in a complicated way as compared to thecase ofthe unicast. Many solutions for the unicastsare not effective with multicast [7] in allowing a safe connection in a changing areaalso as the protection against a particular attacks and threats. There should be a separate infrastructure and plans for security.[9] In this paper we will highlight the security architecture designand feature analysis, as well as factors of insecurity, security threats and the relationship betweenthem in MANET. Security challenges are considered obstacles, for they are threatening thesecurity of MANET network, and there are several challenges facing the security of MANET.

2.2 Attacks (including list of various attacks and definitions)

The attacks can be categorized on the basis of behavior of the attack i.e. Passive or Active attack[8].

2.2.1) Passive attacks:A passive attack does not alter the data transmitted within the network. But it includes theunauthorized “listening” to the network traffic or accumulates data from it. Passive attacker does not disrupt theoperation of a routing protocol but attempts to discover the important information from routed traffic.

2.2.2) Active attacks*:* Active attacks are very severe attacks on the network that prevent message flow between the terminals.However active attacks can be internal or external. Active external attacks can be carried out by outside sources that donot belong to the network.

Internal attacks are from malignantterminals which are part of the network, internal attacks aremore severe and hard to detect than external attacks. These attacks generate unauthorised access to network that helps theattacker to make changes such as modification of packets, DoS, congestion etc.
Active attacks are classified into fourgroups:

2.2.2.1) Dropping Attacks: Compromised terminals or selfish terminals can drop all packets that are not destined for them. Droppingattacks can prevent end-to-end communications between terminals.

2.2.2.2) Modification Attacks: These attacks modify packets and disrupt the overall communication between network terminals.Sinkhole attacks are the example of modification attacks.

2.2.2.3) Fabrication Attacks: In fabrication attack, the attacker send fake message to the neighboring terminals without receivingany related message.
Various Attacks
So here the attacks are categorize into two broad categories: DATAtraffic attacks and CONTROL traffic attacks.

3.1 Data Traffic Attack

Data traffic attack work either in theterminals dropping the data packets while passing through them or in delaying theforwarding of data packets. This includes: Jellyfish and Black hole attack**.**

3.1.1 Jelly Fish

Attackers are always trying to modify messages or generate false messages and thus take down the network's operations which causedenial of service in MANETs. In this section we summary introduce JELLY FISH Attack.Tremendous progress has been made in order to ad hoc networks by developing secure routing protocols that ensure different securityconcepts such as authentication and data integrity.
Moreover, intrusion detection and trust-based systems have been developed to protectMANETs against misbehaviors such as rushing attack, query flood attacks, and selfish behaviors.
Yet, most of the defense mechanisms arenot able to detect a set of protocol compliant attacks called jellyfish (JF) attacks.Jelly fish attack is a type of denials of service attack and also it is a type of the passive attack so it is difficult to find out. It creates delay beforetransmission and the reception of the data packets in network. Applications likeFTP, HTTP, and video conferencing are given by the UDPandTCP. Jelly fish attack interrupts the performance of both protocols [7].

Jellyfish Attack Classification

Jellyfish attack is classified into three categories:

- Jellyfish periodic dropping attack.
- Jellyfish recorder attack.
- Jellyfish Delay variance attack.

Jellyfish attack is categorized as Jelly fish reorderattack, JF periodic dropping attack and JF delayvariance attack. Jelly fish attacks are aimed against the closed loop flows. TCP has well known susceptibilities to drop,delay and mis-order thepackets. Because of this the terminals can alter the sequenceof packets also it dropsfew of the datapackets. Theterminals of jelly fish attacker fully follow the protocol rules therefore this attack is known as a passiveattack.

3.1.2 Blackhole

They analyze the delivery ratio of packet for the multicast sessions in theblackhole attacks. In this the attacker first implements the rushing attacks to achieve the access to the routing mesh, and later it drops all the data packets thatit receives. The delay of processing of the authorizedterminals is set at 20 msas they examined severalschemes by differing number of senders,the number of attackers,the number of receivers, andtheir positions.In paper [3] it is shown a new methoddepended on assuring the best possible path by the use of second path.

In this method, as when a source terminal receives the RREP packets, then it forwards a packet of confirmation via the second best possible path to destination and demanded the destination terminal for whether there is a route to RREP generator or to Next_Hop_Terminal of the RREP generator or not. And if the destination terminal has no route for theseterminals, then both the RREP generator and its Next_Hop_Terminal will consider as malignant terminals. By the use of this method the source terminal can find out the cooperative malignant terminals. Someone in case of two or more cooperative malignantterminal, this methodcannot find out all themalignantterminals.

3.2 Control Traffic Attack

As there is no compulsion in combining thenetwork, malignantterminalmaylink and disorganize thenetwork by seizing thecontrol on the routing tables or via bypassing the valid routes. It may also overhear in network if the terminal can be establish itself as a shortest route to thedestination by applying the unprotected protocols of routing.However there may be other types of attack, like as jamming attacksthat is not a CONTROL attack [4].

This includes DOS attack :

3.2.1 DoS

Denial of service (DoS) attacks is becoming a huge threat to the current networks of computer. PreviousDoS attacks were like technical games that are played among the underground attackers. Like an attacker might wish to achieve the control on an IRC channel throughtheDoS attacks against the owner of the channel. Then the attackers could get theidentification incovered community through taking down thefamous web sites.Attackers thenendangeredthe online businesses with theDoS attacks and are askedfor the payments for giving protection.

Well known attacks of DoS in the Internet normallydefeat the goal by exhausting their resources, whichmay be anything that isassociate to the computingnetwork and performance of the service, like the link bandwidth, application/service buffer,TCP connection buffers, CPU cycles, etc.

Every attacker may also achievesusceptibility, divided into the target servers, and then getthe servicesdown. As it is complicated for the attackers to overburden the resource of the target from the single computer, then severalcurrent attacks of DoS were startedthrough a huge number of the distributed hostsattacking in Internet. These types of attacks are known asthe distributed denial of service (DDoS) attacks.

4.Literature Review

As far as now it is discussedbriefly the challenges of security in the MANET and showsfew analytics inthem. In this portionit isrepresentedan open research problem.Routing information methods are appropriate in all the types of the MANET. In this method, thedecreasing overhead of packet and their processing time, instead of raisingthe accuracy is a significantissue. With the increase in the accuracy, it mayfind out the cooperative malignantterminals. With the decrease in the processing timeof this method the flexibility of MANET will also increase. Redundancy methodcreates a lot of redundant packets and useless resources of terminals.

And also it raises packet lost andcongestion. Efficientlyselecting the number of redundant paths, dependent on the level of risk, is widely challengeable. Also themerging of this method with some other methods to find out themalignantterminals is another challengeable problem.Dynamic frequency is efficient in the multi-type MANETs. By the use of this method in the multi-typeMANET, everyterminalprotects its packets by forwarding in separate frequencies. Additionally, by breaking any one frequency has not effect on the others. This is anissue in this method.

In paper [5] it is explainedseveral types of attacks on a MANETrelated to various layers of MANET and also some available techniques of attack detection are discussed here. A precise idea related to theJellyFish attack is also mentioned in this paper. The suggestedmodel in paper [6] protects the AODV by the use of sequential aggregate signatures (SAS) depended on the RSA and also safelycreated the session key for terminals in MANET to protect the TCP.

5. Conclusion

In any type of communications system, some challengesare there and these types of challenges are taken as anindicator of security gaps thatcreated a weakness in system security and are susceptible to the attacks. The network of MANET, as like the other networks, suffersfew challenges which have been analyzed in this paper. They create a gap in firewall to the MANET. Though, the solutions of security ought to be found to provide the help get out of or to minimize the problems to secure the MANETand increase the level of security in it. Various solutions have been declared or forward compatible with the issues. This MANET network is dynamicallyexpanding and developing rapidly andcontinuously.

References

[1]. R.Sheikh, M. S. Chande, and D. K. Mishra, "Security issues in MANET:A review," presented at the Seventh International Conference On Wireless And Optical Communications Networks (WOCN),2010.

[2]. Aad and J.P. Hubaux, E.W. Knightly, “Impact of Denial of Service Attacks on Ad Hoc Networks”, IEEE/ACM Transactions on Netwroking,vol.16,pp.791 - 802,Aug2008.

[3]. N.-W. Lo and F.-L. Liu, "A Secure Routing Protocol to Prevent Cooperative Black Hole Attack in MANET," in Intelligent Technologies and Engineering Systems.vol. 234, J. Juang and Y.-C. Huang,Eds., ed: Springer New York, 2013, pp. 59-65.

[4]. Bhattacharyya, Aniruddha, Arnab Banerjee, Dipayan Bose, HimadriNathSaha, and Debika Bhattacharya. "Different types of attacks in Mobile ADHOC Network." arXiv preprint arXiv: 1111.4090 (2011).

[5]. Mohammad Wazid, Rajesh Kumar Singh, R. H. Goudar, “ A Survey of Attacks Happened at Different Layers of Mobile Ad-Hoc Network & Some Available Detection Techniques ”, Proceedings published by International Journal of Computer Applications (IJCA) International Conference on Computer Communication and Networks CSI- COMNET-Dec 2011.

[6]. UttamGhosh, Raja Datta, “Identity based Secure AODV and TCP for Mobile Ad Hoc Networks”, Proceedings of ACM ACWR ’11, December 18 - 21 2011.

[7]. Hetal P. Patel, Prof. Minubhai. B. Chaudhari, "Survey: Impact of Jellyfish On Wireless Ad-Hoc Network", in proceeding of INJCR’10, Volume.10, issue.5, no.2pp. 5-9, 2010.

[8]. Gagandeep, Aashima and Pawan Kumar “Analysis of Different Security Attacks in MANETs on Protocol Stack”. International Journal of Engineering and Advanced Technology (IJEAT), Volume-1, Issue-5, June 2012.

[9]. Sneha U. Agalawe ,NitinR.Chopde, (2014) “Security Issues: The Big Challenge In Manet”, International Journal of Computer Science and Mobile Computing ,Vol.3 ,Issue.3, pp. 30-34.

[10]. Djenouri, D., &Badache, N. (2010). Security in mobile ad hoc networks.Germany: LAP LampertAcademic Publishing.